ID: 433429
Sample Name:
ws8W4yPAvg.exe
Cookbook: default.jbs
Time: 19:57:10
Date: 11/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

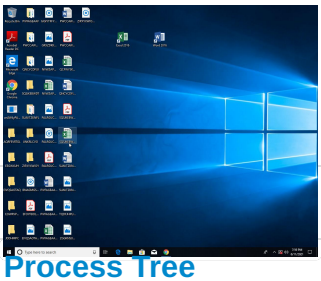
Analysis Report ws8W4yPAvg.exe

Overview

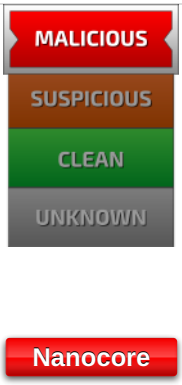
General Information

Sample Name:	ws8W4yPAvg.exe
Analysis ID:	433429
MD5:	4f777ac67c52be4..
SHA1:	f4fe647fa467ba0…
SHA256:	d112e19d34e88c..
Tags:	exe NanoCore RAT
Infos:	

Most interesting Screenshot:



Detection



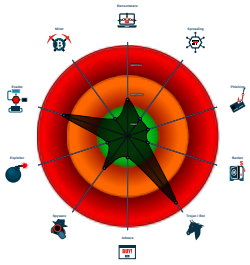
Nanocore

Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Antivirus detection for dropped file
- Detected Nanocore Rat
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for doma…
- Sigma detected: NanoCore
- Snort IDS alert for network traffic (e.…
- Yara detected Nanocore RAT
- .NET source code contains potentia…
- C2 URLs / IPs found in malware con…
- Hides that the sample has been dow…

Classification



Process Tree

- **System is w10x64**
- ws8W4yPAvg.exe (PID: 4088 cmdline: 'C:\Users\user\Desktop\ws8W4yPAvg.exe' MD5: 4F777AC67C52BE4D6A8B6F125BC94661)
  - schtasks.exe (PID: 5292 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor' /xml 'C:\Users\user\AppData\Local\Temp\tmpEFD2.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 6096 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - schtasks.exe (PID: 3708 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor Task' /xml 'C:\Users\user\AppData\Local\Temp\tmpFE1B.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 5396 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- ws8W4yPAvg.exe (PID: 3012 cmdline: C:\Users\user\Desktop\ws8W4yPAvg.exe 0 MD5: 4F777AC67C52BE4D6A8B6F125BC94661)
- dhcpmon.exe (PID: 3216 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' 0 MD5: 4F777AC67C52BE4D6A8B6F125BC94661)
- dhcpmon.exe (PID: 3528 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' MD5: 4F777AC67C52BE4D6A8B6F125BC94661)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "c01ec2cb-25ef-4fd8-a41e-f0012551",
  "Group": "Default",
  "Domain1": "4.tcp.ngrok.io",
  "Domain2": "127.0.0.1",
  "Port": 10877,
  "RunOnStartup": "Enable",
  "RequestElevation": "Enable",
  "BypassUAC": "Enable",
  "ClearZoneIdentifier": "Enable",
  "ClearAccessControl": "Enable",
  "SetCriticalProcess": "Enable",
  "PreventSystemSleep": "Enable",
  "ActivateAwayMode": "Enable",
  "EnableDebugMode": "Disable",
  "RunDelay": 0,
  "ConnectDelay": 4000,
  "RestartDelay": 5000,
  "TimeoutInterval": 5000,
  "KeepAliveTimeout": 30000,
  "MutexTimeout": 5000,
  "LanTimeout": 2500,
  "WanTimeout": 8000,
  "BufferSize": "ffff0000",
  "MaxPacketSize": "0000a000",
  "GCThreshold": "0000a000",
  "UseCustomDNS": "Enable",
  "PrimaryDNSServer": "8.8.8.8",
  "BackupDNSServer": "8.8.4.4",
  "BypassUserAccountControlData": "<?xml version=\"1.0\" encoding=\"UTF-16\"?>\r\n<Task version=\"1.2\" xmlns=\"http://schemas.microsoft.com/windows/2004/02/mit/task\">\r\n
<RegistrationInfo />\r\n  <Triggers />\r\n  <Principals>\r\n    <Principal id=\"Author\">\r\n      <LogonType>InteractiveToken</LogonType>\r\n
<RunLevel>HighestAvailable</RunLevel>\r\n    </Principal>\r\n  </Principals>\r\n  <Settings>\r\n    <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>\r\n
<DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>\r\n    <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>\r\n
<AllowHardTerminate>true</AllowHardTerminate>\r\n    <StartWhenAvailable>false</StartWhenAvailable>\r\n    <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>\r\n
<IdleSettings>\r\n      <StopOnIdleEnd>false</StopOnIdleEnd>\r\n      <RestartOnIdle>false</RestartOnIdle>\r\n    </IdleSettings>\r\n
<AllowStartOnDemand>true</AllowStartOnDemand>\r\n    <Enabled>true</Enabled>\r\n    <Hidden>false</Hidden>\r\n    <RunOnlyIfIdle>false</RunOnlyIfIdle>\r\n
<WakeToRun>false</WakeToRun>\r\n    <ExecutionTimeLimit>PT0S</ExecutionTimeLimit>\r\n    <Priority>4</Priority>\r\n  </Settings>\r\n  <Actions Context=\"Author\">\r\n
<Exec>\r\n      <Command>\"#EXECUTABLEPATH\"</Command>\r\n      <Arguments>$(Arg0)</Arguments>\r\n    </Exec>\r\n  </Actions>\r\n</Task"
}
```


Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
ws8W4yPAvg.exe	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
ws8W4yPAvg.exe	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xff05:$x1: NanoCore Client.exe • 0x1018d:$x2: NanoCore.ClientPluginHost • 0x117c6:$s1: PluginCommand • 0x117ba:$s2: FileCommand • 0x1266b:$s3: PipeExists • 0x18422:$s4: PipeCreated • 0x101b7:$s5: IClientLoggingHost
ws8W4yPAvg.exe	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
ws8W4yPAvg.exe	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfef5:$a: NanoCore • 0xff05:$a: NanoCore • 0x10139:$a: NanoCore • 0x1014d:$a: NanoCore • 0x1018d:$a: NanoCore • 0xff54:$b: ClientPlugin • 0x10156:$b: ClientPlugin • 0x10196:$b: ClientPlugin • 0x1007b:$c: ProjectData • 0x10a82:$d: DESCrypto • 0x1844e:$e: KeepAlive • 0x1643c:$g: LogClientMessage • 0x12637:$i: get_Connected • 0x10db8:$j: #=q • 0x10de8:$j: #=q • 0x10e04:$j: #=q • 0x10e34:$j: #=q • 0x10e50:$j: #=q • 0x10e6c:$j: #=q • 0x10e9c:$j: #=q • 0x10eb8:$j: #=q

Dropped Files

Source	Rule	Description	Author	Strings
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xff05:$x1: NanoCore Client.exe • 0x1018d:$x2: NanoCore.ClientPluginHost • 0x117c6:$s1: PluginCommand • 0x117ba:$s2: FileCommand • 0x1266b:$s3: PipeExists • 0x18422:$s4: PipeCreated • 0x101b7:$s5: IClientLoggingHost
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfef5:$a: NanoCore • 0xff05:$a: NanoCore • 0x10139:$a: NanoCore • 0x1014d:$a: NanoCore • 0x1018d:$a: NanoCore • 0xff54:$b: ClientPlugin • 0x10156:$b: ClientPlugin • 0x10196:$b: ClientPlugin • 0x1007b:$c: ProjectData • 0x10a82:$d: DESCrypto • 0x1844e:$e: KeepAlive • 0x1643c:$g: LogClientMessage • 0x12637:$i: get_Connected • 0x10db8:$j: #=q • 0x10de8:$j: #=q • 0x10e04:$j: #=q • 0x10e34:$j: #=q • 0x10e50:$j: #=q • 0x10e6c:$j: #=q • 0x10e9c:$j: #=q • 0x10eb8:$j: #=q

Memory Dumps

Source	Rule	Description	Author	Strings
00000005.00000002.223088157.000000000052000.00000002.00020000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000005.00000002.223088157.000000000052000.00000002.00020000.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000005.00000002.223088157.000000000052000.00000002.00020000.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfcf5:$a: NanoCore • 0xfd05:$a: NanoCore • 0xff39:$a: NanoCore • 0xff4d:$a: NanoCore • 0xff8d:$a: NanoCore • 0xfd54:$b: ClientPlugin • 0xff56:$b: ClientPlugin • 0xff96:$b: ClientPlugin • 0xfe7b:$c: ProjectData • 0x10882:$d: DESCrypto • 0x1824e:$e: KeepAlive • 0x1623c:$g: LogClientMessage • 0x12437:$i: get_Connected • 0x10bb8:$j: #=q • 0x10be8:$j: #=q • 0x10c04:$j: #=q • 0x10c34:$j: #=q • 0x10c50:$j: #=q • 0x10c6c:$j: #=q • 0x10c9c:$j: #=q • 0x10cb8:$j: #=q
00000000.00000002.464501359.000000000062000.00000002.00020000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000000.00000002.464501359.000000000062000.00000002.00020000.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
Click to see the 43 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings

Source	Rule	Description	Author	Strings
8.0.dhcpmon.exe.c0000.0.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
8.0.dhcpmon.exe.c0000.0.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xff05:$x1: NanoCore Client.exe • 0x1018d:$x2: NanoCore.ClientPluginHost • 0x117c6:$s1: PluginCommand • 0x117ba:$s2: FileCommand • 0x1266b:$s3: PipeExists • 0x18422:$s4: PipeCreated • 0x101b7:$s5: IClientLoggingHost
8.0.dhcpmon.exe.c0000.0.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
8.0.dhcpmon.exe.c0000.0.unpack	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfef5:$a: NanoCore • 0xff05:$a: NanoCore • 0x10139:$a: NanoCore • 0x1014d:$a: NanoCore • 0x1018d:$a: NanoCore • 0xff54:$b: ClientPlugin • 0x10156:$b: ClientPlugin • 0x10196:$b: ClientPlugin • 0x1007b:$c: ProjectData • 0x10a82:$d: DESCrypto • 0x1844e:$e: KeepAlive • 0x1643c:$g: LogClientMessage • 0x12637:$i: get_Connected • 0x10db8:$j: #=q • 0x10de8:$j: #=q • 0x10e04:$j: #=q • 0x10e34:$j: #=q • 0x10e50:$j: #=q • 0x10e6c:$j: #=q • 0x10e9c:$j: #=q • 0x10eb8:$j: #=q
7.2.dhcpmon.exe.390000.0.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
Click to see the 72 entries				

Sigma Overview

AV Detection:

Sigma detected: NanoCore

E-Banking Fraud:

Sigma detected: NanoCore

Stealing of Sensitive Information:

Sigma detected: NanoCore

Remote Access Functionality:

Sigma detected: NanoCore

Signature Overview

Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

Antivirus detection for dropped file

Found malware configuration

Multi AV Scanner detection for domain / URL

Yara detected Nanocore RAT

Machine Learning detection for dropped file

Machine Learning detection for sample

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected Nanocore RAT

Operating System Destruction:

Protects its processes via BreakOnTermination flag

System Summary:

Malicious sample detected (through community Yara rule)

Data Obfuscation:

.NET source code contains potential unpacker

Boot Survival:

Uses schtasks.exe or at.exe to add and modify task schedules

Hooking and other Techniques for Hiding and Protection:

Hides that the sample has been downloaded from the Internet (zone.identifier)

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

Detected Nanocore Rat

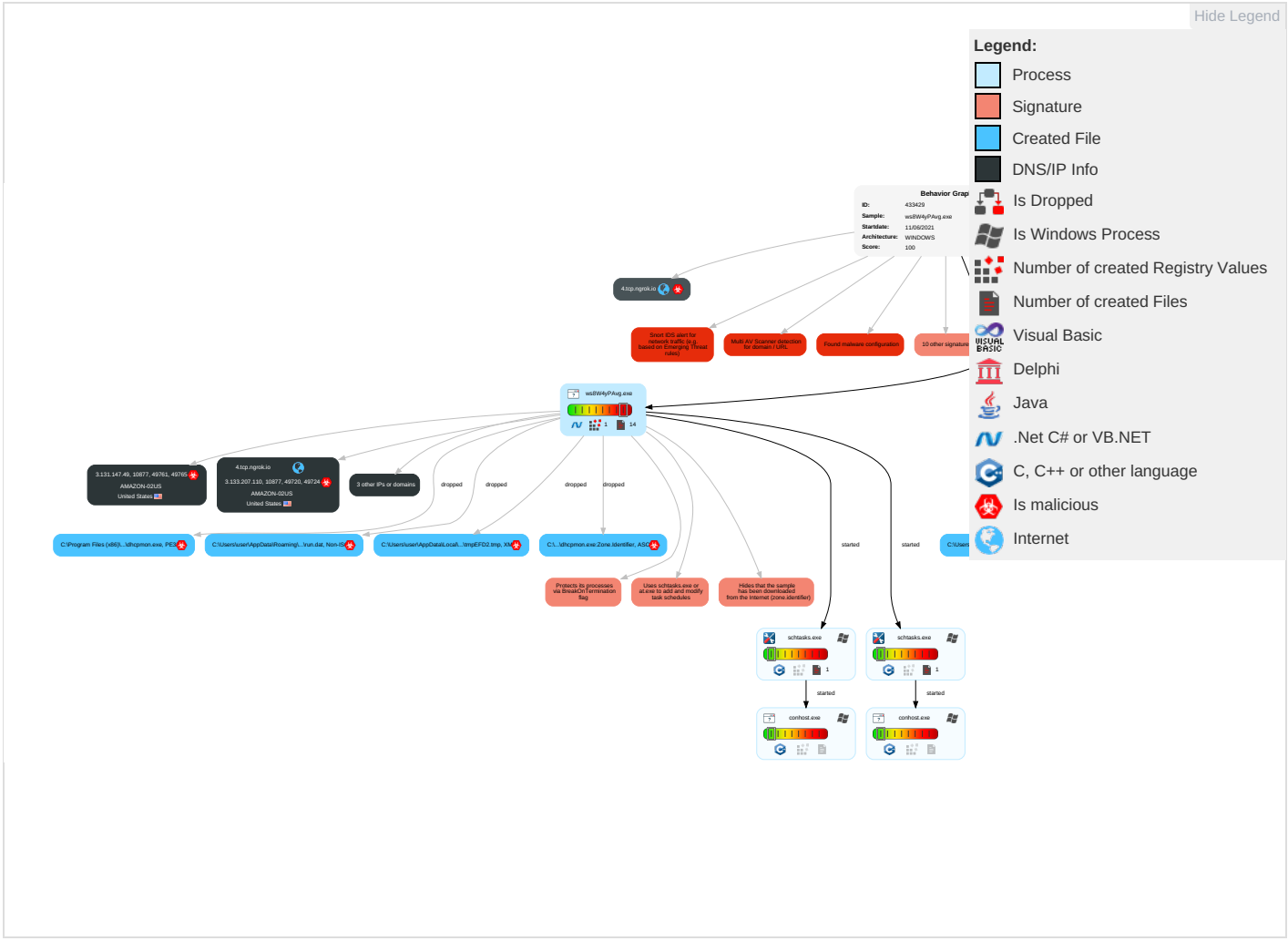
Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Scheduled Task/Job 1	Scheduled Task/Job 1	Process Injection 1 2	Masquerading 2	Input Capture 2 1	Security Software Discovery 1	Remote Services	Input Capture 2 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdro Insecure Network Commun

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Disable or Modify Tools 1	LSASS Memory	Process Discovery 2	Remote Desktop Protocol	Archive Collected Data 1 1	Exfiltration Over Bluetooth	Non-Standard Port 1	Exploit S Redirect Calls/SM
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 2 1	Security Account Manager	Virtualization/Sandbox Evasion 2 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Remote Access Software 1	Exploit S Track De Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 2	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 1	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	System Information Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 1 1	Manipula Device Commun
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Hidden Files and Directories 1	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 1	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue W Access P
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Software Packing 1 2	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgra Insecure Protocols

Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
ws8W4yPAvg.exe	100%	Avira	TR/Dropper.MSIL.Gen7	
ws8W4yPAvg.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	100%	Avira	TR/Dropper.MSIL.Gen7	
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	100%	Joe Sandbox ML		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.0.ws8W4yPAvg.exe.50000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
7.0.dhcpmon.exe.390000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
8.0.dhcpmon.exe.c0000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
7.2.dhcpmon.exe.390000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
8.2.dhcpmon.exe.c0000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
5.2.ws8W4yPAvg.exe.50000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
0.2.ws8W4yPAvg.exe.60000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
0.0.ws8W4yPAvg.exe.60000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Domains

Source	Detection	Scanner	Label	Link
4.tcp.ngrok.io	12%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
4.tcp.ngrok.io	12%	Virustotal		Browse
4.tcp.ngrok.io	0%	Avira URL Cloud	safe	
127.0.0.1	0%	Virustotal		Browse
127.0.0.1	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
4.tcp.ngrok.io	3.133.207.110	true	true	• 12%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
4.tcp.ngrok.io	true	• 12%, Virustotal, Browse • Avira URL Cloud: safe	unknown
127.0.0.1	true	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
3.131.147.49	unknown	United States		16509	AMAZON-02US	true
3.133.207.110	4.tcp.ngrok.io	United States		16509	AMAZON-02US	true
3.22.15.135	unknown	United States		16509	AMAZON-02US	true

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	433429
Start date:	11.06.2021
Start time:	19:57:10
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 15s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	ws8W4yPAvg.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	29
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@10/8@14/5
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
19:57:58	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
19:58:01	Task Scheduler	Run new task: DHCP Monitor path: "C:\Users\user\Desktop\ws8W4yPAvg.exe" s>$(Arg0)
19:58:02	API Interceptor	990x Sleep call for process: ws8W4yPAvg.exe modified
19:58:03	Task Scheduler	Run new task: DHCP Monitor Task path: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" s>$(Arg0)

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
3.131.147.49	FiYBg9R8m0.exe	Get hash	malicious	Browse	
	ooAUh9ba7E.exe	Get hash	malicious	Browse	
	A6FAm1ae1j.exe	Get hash	malicious	Browse	
	vZvmgrCXam.exe	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	63C2AB0ECE24B47CDCFE2128789214F87451A3D8 2D641.exe	Get hash	malicious	Browse	
	DC8DDCD4DB035FA647001A01CAB6A2866D092FCA AD182.exe	Get hash	malicious	Browse	
	tmkfdBpwAx.exe	Get hash	malicious	Browse	
	LGKacQbjeH.exe	Get hash	malicious	Browse	
	qiCot2DU55.exe	Get hash	malicious	Browse	
	YZJfsPAFBJ.exe	Get hash	malicious	Browse	
	T91uHSVq.exe	Get hash	malicious	Browse	
	aYqoy7xF7y.exe	Get hash	malicious	Browse	
	Krtw4Kl87V.exe	Get hash	malicious	Browse	
	YFZX6dTsiT.exe	Get hash	malicious	Browse	
	vzcJbGFs.exe	Get hash	malicious	Browse	
	rQMm2jZD.exe	Get hash	malicious	Browse	
	PsbfBdoToY.exe	Get hash	malicious	Browse	
	BcaDguoEzV.exe	Get hash	malicious	Browse	
	eSJ6Q8F2.exe	Get hash	malicious	Browse	
	BwQRSJm1.exe	Get hash	malicious	Browse	
3.133.207.110	FiYBg9R8m0.exe	Get hash	malicious	Browse	
	BWAlL8lrQb.exe	Get hash	malicious	Browse	
	ooAUh9ba7E.exe	Get hash	malicious	Browse	
	A6FAm1ae1j.exe	Get hash	malicious	Browse	
	CpOFmSHBGH.exe	Get hash	malicious	Browse	
	63C2AB0ECE24B47CDCFE2128789214F87451A3D8 2D641.exe	Get hash	malicious	Browse	
	D3AAB88BB737961C971ED047B4C2D5B640EFF8E6 78781.exe	Get hash	malicious	Browse	
	DC8DDCD4DB035FA647001A01CAB6A2866D092FCA AD182.exe	Get hash	malicious	Browse	
	tmkfdBpwAx.exe	Get hash	malicious	Browse	
	J6wDHe2QdA.exe	Get hash	malicious	Browse	
	LGKacQbjeH.exe	Get hash	malicious	Browse	
	qiCot2DU55.exe	Get hash	malicious	Browse	
	YZJfsPAFBJ.exe	Get hash	malicious	Browse	
	aYqoy7xF7y.exe	Get hash	malicious	Browse	
	zOlLBCUG9R.exe	Get hash	malicious	Browse	
	YFZX6dTsiT.exe	Get hash	malicious	Browse	
	vzcJbGFs.exe	Get hash	malicious	Browse	
	rQMm2jZD.exe	Get hash	malicious	Browse	
	43SjNv5s.exe	Get hash	malicious	Browse	
	mNxVbma4uT.exe	Get hash	malicious	Browse	
3.22.15.135	ehDnx4Ke5d.exe	Get hash	malicious	Browse	
	BWAlL8lrQb.exe	Get hash	malicious	Browse	
	H4Q0l1RIuW.exe	Get hash	malicious	Browse	
	ooAUh9ba7E.exe	Get hash	malicious	Browse	
	CpOFmSHBGH.exe	Get hash	malicious	Browse	
	GBtiwIB30h.exe	Get hash	malicious	Browse	
	vZvmgrCXam.exe	Get hash	malicious	Browse	
	D3AAB88BB737961C971ED047B4C2D5B640EFF8E6 78781.exe	Get hash	malicious	Browse	
	DC8DDCD4DB035FA647001A01CAB6A2866D092FCA AD182.exe	Get hash	malicious	Browse	
	tmkfdBpwAx.exe	Get hash	malicious	Browse	
	J6wDHe2QdA.exe	Get hash	malicious	Browse	
	LGKacQbjeH.exe	Get hash	malicious	Browse	
	qiCot2DU55.exe	Get hash	malicious	Browse	
	YZJfsPAFBJ.exe	Get hash	malicious	Browse	
	TBjxmaP9.exe	Get hash	malicious	Browse	
	Krtw4Kl87V.exe	Get hash	malicious	Browse	
	YFZX6dTsiT.exe	Get hash	malicious	Browse	
	sz.exe	Get hash	malicious	Browse	
	vzcJbGFs.exe	Get hash	malicious	Browse	
	mNxVbma4uT.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
4.tcp.ngrok.io	ehDnx4Ke5d.exe	Get hash	malicious	Browse	• 3.138.180.119
	XQehPgTn35.exe	Get hash	malicious	Browse	• 3.138.180.119
	FiYBg9R8m0.exe	Get hash	malicious	Browse	• 3.133.207.110
	BWAlL8lrQb.exe	Get hash	malicious	Browse	• 3.129.187.220
	0BFE93ABC8B3801B7E906960F6D69CC51088B76544EFC.exe	Get hash	malicious	Browse	• 3.138.180.119
	H4Q0l1RIuW.exe	Get hash	malicious	Browse	• 3.129.187.220
	ooAUh9ba7E.exe	Get hash	malicious	Browse	• 3.133.207.110
	A6FAm1ae1j.exe	Get hash	malicious	Browse	• 3.133.207.110
	CpOFmSHBGH.exe	Get hash	malicious	Browse	• 3.133.207.110
	GBtiwIB30h.exe	Get hash	malicious	Browse	• 3.22.15.135
	vZvmgrCXam.exe	Get hash	malicious	Browse	• 3.138.180.119
	63C2AB0ECE24B47CDCFE2128789214F87451A3D82D641.exe	Get hash	malicious	Browse	• 3.136.65.236
	D3AAB88BB737961C971ED047B4C2D5B640EFF8E678781.exe	Get hash	malicious	Browse	• 3.22.15.135
	DC8DDCD4DB035FA647001A01CAB6A2866D092FCAAD182.exe	Get hash	malicious	Browse	• 3.129.187.220
	tmkfdBpwAx.exe	Get hash	malicious	Browse	• 3.131.147.49
	J6wDHe2QdA.exe	Get hash	malicious	Browse	• 3.136.65.236
	LGKacQbjeH.exe	Get hash	malicious	Browse	• 3.138.180.119
	qiCot2DU55.exe	Get hash	malicious	Browse	• 3.136.65.236
	yEh8mVeLA6.exe	Get hash	malicious	Browse	• 3.136.65.236
	XFdEhEAPeE.exe	Get hash	malicious	Browse	• 3.136.65.236

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AMAZON-02US	UOMp9cDcqZ.exe	Get hash	malicious	Browse	• 52.58.78.16
	OrderKLB210568.exe	Get hash	malicious	Browse	• 34.215.126.147
	q7jxy6gZMb.exe	Get hash	malicious	Browse	• 104.192.141.1
	b9f5bca9a22f08aad48674bc42e4eaf72ab8aa3d652ba.exe	Get hash	malicious	Browse	• 52.219.158.14
	8BDBD0yy0q.apk	Get hash	malicious	Browse	• 52.17.153.103
	8BDBD0yy0q.apk	Get hash	malicious	Browse	• 13.224.195.88
	ehDnx4Ke5d.exe	Get hash	malicious	Browse	• 3.22.15.135
	KY4cmAI0jU.exe	Get hash	malicious	Browse	• 3.34.12.41
	c71fd2gJus.exe	Get hash	malicious	Browse	• 52.219.64.3
	XQehPgTn35.exe	Get hash	malicious	Browse	• 3.136.65.236
	E1a92ARmPw.exe	Get hash	malicious	Browse	• 35.157.179.180
	crt9O3URua.exe	Get hash	malicious	Browse	• 35.157.179.180
	E1a92ARmPw.exe	Get hash	malicious	Browse	• 52.218.105.219
	DNPr7t0GMY.exe	Get hash	malicious	Browse	• 13.59.53.244
	ITAPQJikGw.exe	Get hash	malicious	Browse	• 99.83.154.118
	SKlGhwkzTi.exe	Get hash	malicious	Browse	• 44.227.65.245
	SecuriteInfo.com.Trojan.Packed2.43183.29557.exe	Get hash	malicious	Browse	• 13.59.53.244
	Letter 1019.xlsx	Get hash	malicious	Browse	• 18.140.1.169
	#U260e#Ufe0f Zeppelin.com AudioMessage_259-55.HTM	Get hash	malicious	Browse	• 143.204.98.37
	Proforma Invoice and Bank swift-REG.PI-0086547654.exe	Get hash	malicious	Browse	• 75.2.26.18
AMAZON-02US	UOMp9cDcqZ.exe	Get hash	malicious	Browse	• 52.58.78.16
	OrderKLB210568.exe	Get hash	malicious	Browse	• 34.215.126.147
	q7jxy6gZMb.exe	Get hash	malicious	Browse	• 104.192.141.1
	b9f5bca9a22f08aad48674bc42e4eaf72ab8aa3d652ba.exe	Get hash	malicious	Browse	• 52.219.158.14
	8BDBD0yy0q.apk	Get hash	malicious	Browse	• 52.17.153.103
	8BDBD0yy0q.apk	Get hash	malicious	Browse	• 13.224.195.88
	ehDnx4Ke5d.exe	Get hash	malicious	Browse	• 3.22.15.135
	KY4cmAI0jU.exe	Get hash	malicious	Browse	• 3.34.12.41
	c71fd2gJus.exe	Get hash	malicious	Browse	• 52.219.64.3
	XQehPgTn35.exe	Get hash	malicious	Browse	• 3.136.65.236
	E1a92ARmPw.exe	Get hash	malicious	Browse	• 35.157.179.180
	crt9O3URua.exe	Get hash	malicious	Browse	• 35.157.179.180
	E1a92ARmPw.exe	Get hash	malicious	Browse	• 52.218.105.219
	DNPr7t0GMY.exe	Get hash	malicious	Browse	• 13.59.53.244
	ITAPQJikGw.exe	Get hash	malicious	Browse	• 99.83.154.118
	SKlGhwkzTi.exe	Get hash	malicious	Browse	• 44.227.65.245
	SecuriteInfo.com.Trojan.Packed2.43183.29557.exe	Get hash	malicious	Browse	• 13.59.53.244

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Letter 1019.xlsx	Get hash	malicious	Browse	• 18.140.1.169
	#U260e#Ufe0f Zeppelin.com AudioMessage_259-55.HTM	Get hash	malicious	Browse	• 143.204.98.37
	Proforma Invoice and Bank swift-REG.PI-0086547654.exe	Get hash	malicious	Browse	• 75.2.26.18
AMAZON-02US	UOMp9cDcqZ.exe	Get hash	malicious	Browse	• 52.58.78.16
	OrderKLB210568.exe	Get hash	malicious	Browse	• 34.215.126.147
	q7jxy6gZMb.exe	Get hash	malicious	Browse	• 104.192.141.1
	b9f5bca9a22f08aad48674bc42e4eaf72ab8aa3d652ba.exe	Get hash	malicious	Browse	• 52.219.158.14
	8BDBD0yy0q.apk	Get hash	malicious	Browse	• 52.17.153.103
	8BDBD0yy0q.apk	Get hash	malicious	Browse	• 13.224.195.88
	ehDnx4Ke5d.exe	Get hash	malicious	Browse	• 3.22.15.135
	KY4cmAI0jU.exe	Get hash	malicious	Browse	• 3.34.12.41
	c71fd2gJus.exe	Get hash	malicious	Browse	• 52.219.64.3
	XQehPgTn35.exe	Get hash	malicious	Browse	• 3.136.65.236
	E1a92ARmPw.exe	Get hash	malicious	Browse	• 35.157.179.180
	crt9O3URua.exe	Get hash	malicious	Browse	• 35.157.179.180
	E1a92ARmPw.exe	Get hash	malicious	Browse	• 52.218.105.219
	DNPr7t0GMY.exe	Get hash	malicious	Browse	• 13.59.53.244
	ITAPQJikGw.exe	Get hash	malicious	Browse	• 99.83.154.118
	SKlGhwkzTi.exe	Get hash	malicious	Browse	• 44.227.65.245
	SecuriteInfo.com.Trojan.Packed2.43183.29557.exe	Get hash	malicious	Browse	• 13.59.53.244
	Letter 1019.xlsx	Get hash	malicious	Browse	• 18.140.1.169
	#U260e#Ufe0f Zeppelin.com AudioMessage_259-55.HTM	Get hash	malicious	Browse	• 143.204.98.37
	Proforma Invoice and Bank swift-REG.PI-0086547654.exe	Get hash	malicious	Browse	• 75.2.26.18

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe

Process:	C:\Users\user\Desktop\ws8W4yPAvg.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	207872
Entropy (8bit):	7.449363749668439
Encrypted:	false
SSDEEP:	6144:MLV6Bta6dtJmakIM5A6fA+eXcTTacsRy3Cj+R:MLV6BtpmkxuA+eXsaDCUq
MD5:	4F777AC67C52BE4D6A8B6F125BC94661
SHA1:	F4FE647FA467BA0D039F9CA61BC18583734F7B46
SHA-256:	D112E19D34E88C040A70367143569C965CB48DBB1FA36579838C51F8CA9EBE7C
SHA-512:	55009C93CBEAA16712DA32025E7B6ED97ED4184F8EF044C46C2F6A7B2692733DC46679BD3124CD8F5CA69884D590DD2401469BBBC0A51D82A8E5219A565409C
Malicious:	**true**
Yara Hits:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....'.T.....b..... .....@.. ....8...W.... ..._..... ....H.....text..... ....`.reloc.....@..B.rsrc...._... ...`.....@..@.....t.....H.....T.....0..Q.....o5.....*.o6....-.&.....3+..+.... ....3.....1..... 2... ....3.... .....*.*....0..E.....s7....-(&s 8....-&&s9....,$&s:.....s;.....*.....+.....+.....+.....0.....~....o<...*..0.....~....o=...*..0.....~....o>...*..0.....~....o?...*..0.....~....o@...*..0.....-.&(A...*&+...0..$..... ~B.....-.(...+.-.&+..B...+.~B...*.0.....-.&(A...*&+...0..

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe:Zone.Identifier

Process:	C:\Users\user\Desktop\ws8W4yPAvg.exe

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe:Zone.Identifier	
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\dhcpmon.exe.log	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	525
Entropy (8bit):	5.2874233355119316
Encrypted:	false
SSDEEP:	12:Q3LaJU20NaL10U29hJ5g1B0U2ukyrFk70Ug+9Yz9tv:MLF20NaL329hJ5g522rWz2T
MD5:	61CCF53571C9ABA6511D696CB0D32E45
SHA1:	A13A42A20EC14942F52DB20FB16A0A520F8183CE
SHA-256:	3459BDF6C0B7F9D43649ADAAF19BA8D5D133BCBE5EF80CF4B7000DC91E10903B
SHA-512:	90E180D9A681F82C010C326456AC88EBB89256CC769E900BFB4B2DF92E69CA69726863B45DFE4627FC1EE8C281F2AF86A6A1E2EF1710094CCD3F4E092872F06
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Windows.Forms\bd8d59c984c9f5f2695f64341115cdf0\System.Windows.Forms.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.ni.dll",0..

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\ws8W4yPAvg.exe.log	
Process:	C:\Users\user\Desktop\ws8W4yPAvg.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	525
Entropy (8bit):	5.2874233355119316
Encrypted:	false
SSDEEP:	12:Q3LaJU20NaL10U29hJ5g1B0U2ukyrFk70Ug+9Yz9tv:MLF20NaL329hJ5g522rWz2T
MD5:	61CCF53571C9ABA6511D696CB0D32E45
SHA1:	A13A42A20EC14942F52DB20FB16A0A520F8183CE
SHA-256:	3459BDF6C0B7F9D43649ADAAF19BA8D5D133BCBE5EF80CF4B7000DC91E10903B
SHA-512:	90E180D9A681F82C010C326456AC88EBB89256CC769E900BFB4B2DF92E69CA69726863B45DFE4627FC1EE8C281F2AF86A6A1E2EF1710094CCD3F4E092872F06
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Windows.Forms\bd8d59c984c9f5f2695f64341115cdf0\System.Windows.Forms.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.ni.dll",0..

C:\Users\user\AppData\Local\Temp\tmpEFD2.tmp	
Process:	C:\Users\user\Desktop\ws8W4yPAvg.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1300
Entropy (8bit):	5.112502432656558
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0G3xtn:cbk4oL600QydbQxIYODOLedq3rj
MD5:	29AC038EA24283E9A0B7F9AA237F82BA
SHA1:	FA9A6B94A62D82114DC3D3E166752BDCD1CC8585
SHA-256:	DD957BD3A0CCA20FB6AD36B54CEBDC252241F3D770ECB3431C87717B5FE48B7A

C:\Users\user\AppData\Local\Temp\tmpEFD2.tmp	
SHA-512:	3EC9561C4805E224463AD1824F9AC231A12BC2108C79EF5900E7392B52FBDE1BD43B1E4A762FE9DBDB6F44B1F517FC6C3A2721DCFFAFF3CBD02DAF3F1A54F1A8
Malicious:	**true**
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>HighestAvailable</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </IdleSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunOnlyIfIdle>.. <Wak

C:\Users\user\AppData\Local\Temp\tmpFE1B.tmp	
Process:	C:\Users\user\Desktop\ws8W4yPAvg.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1310
Entropy (8bit):	5.109425792877704
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0R3xtn:cbk4oL600QydbQxIYODOLedq3S3j
MD5:	5C2F41CFC6F988C859DA7D727AC2B62A
SHA1:	68999C85FC7E37BAB9216E0099836D40D4545C1C
SHA-256:	98B6E66B6C2173B9B91FC97FE51805340EFDE978B695453742EBAB631018398B
SHA-512:	B5DA5DA378D038AFBF8A7738E47921ED39F9B726E2CAA2993D915D9291A3322F94EFE8CCA6E7AD678A670DB19926B22B20E5028460FCC89CEA7F6635E755733
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>HighestAvailable</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </IdleSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunOnlyIfIdle>.. <Wak

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Users\user\Desktop\ws8W4yPAvg.exe
File Type:	Non-ISO extended-ASCII text, with no line terminators
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:3JBI8tn:5BI8
MD5:	9C5F59B284ADF6282C473111B7B221FF
SHA1:	B307A21EDBB27C8C3B7CC0F2BB8020FA61D2E55A
SHA-256:	9CBE8533F0F928F1232F4A1441B49A1D687738826D3057265D174EB300B7FF3D
SHA-512:	01A70199AB09D7CAF3D37662F4193F49923C5991347D002341C1A260C2517886F2867C65DE083D57047941A5D1357017ACCFDC50948CB366688715FFFA6A2AC1
Malicious:	**true**
Preview:	E...M-.H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	
Process:	C:\Users\user\Desktop\ws8W4yPAvg.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	37
Entropy (8bit):	4.506750662926249
Encrypted:	false
SSDEEP:	3:oNWXp5vSWkczLACn:oNWXpFS8LACn
MD5:	2289D44B878445B8D01E11EA3DC07C63
SHA1:	B229492032E28EF9E89CAAC1B79347DFBC00AB37
SHA-256:	A8B6D4E014D16578BA30B167E59BCA31241E34A19CA6D362E6F21C08B6257FD7
SHA-512:	4C7CC362A46050F0C2B1D41A4C11F5D421E8CCAC425FA83640646960AAFFC3251DA32C8FB8C2524F39BB14CEA8BDD5A87C0E7ADFC77E97217ED8D78EC48C12B
Malicious:	false
Preview:	C:\Users\user\Desktop\ws8W4yPAvg.exe

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.449363749668439
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	ws8W4yPAvg.exe
File size:	207872
MD5:	4f777ac67c52be4d6a8b6f125bc94661
SHA1:	f4fe647fa467ba0d039f9ca61bc18583734f7b46
SHA256:	d112e19d34e88c040a70367143569c965cb48dbb1fa36579838c51f8ca9ebe7c
SHA512:	55009c93cbeaa16712da32025e7b6ed97ed4184f8ef044c46c2f6a7b2692733dc46679bd3124cd8f5ca69884d590dd2401469bbbc0a51d82a8e5219a565409ca
SSDEEP:	6144:MLV6Bta6dtJmakIM5A6fA+eXcTTacsRy3Cj+R:MLV6BtpmkxuA+eXsaDCUq
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....'.T.....b..... .....@.. ....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x41e792
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x54E927A1 [Sun Feb 22 00:49:37 2015 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v2.0.50727
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x1c798	0x1c800	False	0.594503837719	data	6.59804227232	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.reloc	0x20000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
.rsrc	0x22000	0x15fc0	0x16000	False	1.00012207031	data	7.99764484035	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Imports

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
06/11/21-19:58:04.588686	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49720	10877	192.168.2.3	3.133.207.110
06/11/21-19:58:09.044779	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49724	10877	192.168.2.3	3.133.207.110
06/11/21-19:58:14.567289	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49728	10877	192.168.2.3	3.133.207.110
06/11/21-19:58:34.714536	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49738	10877	192.168.2.3	3.133.207.110
06/11/21-19:58:39.400073	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49739	10877	192.168.2.3	3.133.207.110
06/11/21-19:58:44.481466	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49740	10877	192.168.2.3	3.133.207.110
06/11/21-19:59:04.476577	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49750	10877	192.168.2.3	3.22.15.135
06/11/21-19:59:08.898642	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49756	10877	192.168.2.3	3.133.207.110
06/11/21-19:59:14.004266	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49757	10877	192.168.2.3	3.22.15.135
06/11/21-19:59:34.725309	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49761	10877	192.168.2.3	3.131.147.49
06/11/21-19:59:39.481808	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49764	10877	192.168.2.3	3.22.15.135
06/11/21-19:59:44.243284	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49765	10877	192.168.2.3	3.131.147.49
06/11/21-20:00:03.840152	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49769	10877	192.168.2.3	3.138.180.119
06/11/21-20:00:08.194247	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49770	10877	192.168.2.3	3.138.180.119

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 11, 2021 19:58:04.269948006 CEST	192.168.2.3	8.8.8.8	0x63cf	Standard query (0)	4.tcp.ngrok.io	A (IP address)	IN (0x0001)
Jun 11, 2021 19:58:08.838542938 CEST	192.168.2.3	8.8.8.8	0x7f34	Standard query (0)	4.tcp.ngrok.io	A (IP address)	IN (0x0001)
Jun 11, 2021 19:58:14.362339973 CEST	192.168.2.3	8.8.8.8	0xcbc1	Standard query (0)	4.tcp.ngrok.io	A (IP address)	IN (0x0001)
Jun 11, 2021 19:58:34.513066053 CEST	192.168.2.3	8.8.8.8	0xeeb3	Standard query (0)	4.tcp.ngrok.io	A (IP address)	IN (0x0001)
Jun 11, 2021 19:58:39.199907064 CEST	192.168.2.3	8.8.8.8	0xc08f	Standard query (0)	4.tcp.ngrok.io	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 11, 2021 19:58:44.280694962 CEST	192.168.2.3	8.8.8.8	0xc847	Standard query (0)	4.tcp.ngrok.io	A (IP address)	IN (0x0001)
Jun 11, 2021 19:59:03.929529905 CEST	192.168.2.3	8.8.8.8	0x4f2a	Standard query (0)	4.tcp.ngrok.io	A (IP address)	IN (0x0001)
Jun 11, 2021 19:59:08.695753098 CEST	192.168.2.3	8.8.8.8	0xdc18	Standard query (0)	4.tcp.ngrok.io	A (IP address)	IN (0x0001)
Jun 11, 2021 19:59:13.745275021 CEST	192.168.2.3	8.8.8.8	0x61cb	Standard query (0)	4.tcp.ngrok.io	A (IP address)	IN (0x0001)
Jun 11, 2021 19:59:34.521006107 CEST	192.168.2.3	8.8.8.8	0x3add	Standard query (0)	4.tcp.ngrok.io	A (IP address)	IN (0x0001)
Jun 11, 2021 19:59:39.277440071 CEST	192.168.2.3	8.8.8.8	0x1a22	Standard query (0)	4.tcp.ngrok.io	A (IP address)	IN (0x0001)
Jun 11, 2021 19:59:44.040237904 CEST	192.168.2.3	8.8.8.8	0x2764	Standard query (0)	4.tcp.ngrok.io	A (IP address)	IN (0x0001)
Jun 11, 2021 20:00:03.633408070 CEST	192.168.2.3	8.8.8.8	0xfc99	Standard query (0)	4.tcp.ngrok.io	A (IP address)	IN (0x0001)
Jun 11, 2021 20:00:07.992259026 CEST	192.168.2.3	8.8.8.8	0xac89	Standard query (0)	4.tcp.ngrok.io	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 11, 2021 19:58:04.333017111 CEST	8.8.8.8	192.168.2.3	0x63cf	No error (0)	4.tcp.ngrok.io		3.133.207.110	A (IP address)	IN (0x0001)
Jun 11, 2021 19:58:08.899372101 CEST	8.8.8.8	192.168.2.3	0x7f34	No error (0)	4.tcp.ngrok.io		3.133.207.110	A (IP address)	IN (0x0001)
Jun 11, 2021 19:58:14.423520088 CEST	8.8.8.8	192.168.2.3	0xcbc1	No error (0)	4.tcp.ngrok.io		3.133.207.110	A (IP address)	IN (0x0001)
Jun 11, 2021 19:58:34.571826935 CEST	8.8.8.8	192.168.2.3	0xeeb3	No error (0)	4.tcp.ngrok.io		3.133.207.110	A (IP address)	IN (0x0001)
Jun 11, 2021 19:58:39.258991003 CEST	8.8.8.8	192.168.2.3	0xc08f	No error (0)	4.tcp.ngrok.io		3.133.207.110	A (IP address)	IN (0x0001)
Jun 11, 2021 19:58:44.339658976 CEST	8.8.8.8	192.168.2.3	0xc847	No error (0)	4.tcp.ngrok.io		3.133.207.110	A (IP address)	IN (0x0001)
Jun 11, 2021 19:59:03.993848085 CEST	8.8.8.8	192.168.2.3	0x4f2a	No error (0)	4.tcp.ngrok.io		3.22.15.135	A (IP address)	IN (0x0001)
Jun 11, 2021 19:59:08.755603075 CEST	8.8.8.8	192.168.2.3	0xdc18	No error (0)	4.tcp.ngrok.io		3.133.207.110	A (IP address)	IN (0x0001)
Jun 11, 2021 19:59:13.804868937 CEST	8.8.8.8	192.168.2.3	0x61cb	No error (0)	4.tcp.ngrok.io		3.22.15.135	A (IP address)	IN (0x0001)
Jun 11, 2021 19:59:34.579324961 CEST	8.8.8.8	192.168.2.3	0x3add	No error (0)	4.tcp.ngrok.io		3.131.147.49	A (IP address)	IN (0x0001)
Jun 11, 2021 19:59:39.336503029 CEST	8.8.8.8	192.168.2.3	0x1a22	No error (0)	4.tcp.ngrok.io		3.22.15.135	A (IP address)	IN (0x0001)
Jun 11, 2021 19:59:44.100423098 CEST	8.8.8.8	192.168.2.3	0x2764	No error (0)	4.tcp.ngrok.io		3.131.147.49	A (IP address)	IN (0x0001)
Jun 11, 2021 20:00:03.696804047 CEST	8.8.8.8	192.168.2.3	0xfc99	No error (0)	4.tcp.ngrok.io		3.138.180.119	A (IP address)	IN (0x0001)
Jun 11, 2021 20:00:08.053497076 CEST	8.8.8.8	192.168.2.3	0xac89	No error (0)	4.tcp.ngrok.io		3.138.180.119	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: ws8W4yPAvg.exe PID: 4088 Parent PID: 5676

General

Start time:	19:57:56
Start date:	11/06/2021
Path:	C:\Users\user\Desktop\ws8W4yPAvg.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\ws8W4yPAvg.exe'
Imagebase:	0x60000
File size:	207872 bytes
MD5 hash:	4F777AC67C52BE4D6A8B6F125BC94661
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.464501359.0000000000062000.00000002.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.464501359.0000000000062000.00000002.00020000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.464501359.0000000000062000.00000002.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000000.198429567.0000000000062000.00000002.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000000.198429567.0000000000062000.00000002.00020000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000000.198429567.0000000000062000.00000002.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Registry Activities

Show Windows behavior

Key Value Created

Analysis Process: schtasks.exe PID: 5292 Parent PID: 4088

General

Start time:	19:57:58

Start date:	11/06/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'schtasks.exe' /create /f /tn 'DHCP Monitor' /xml 'C:\Users\user\AppData\Local\Temp\tmpEFD2.tmp'
Imagebase:	0x8d0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

File Read

Analysis Process: conhost.exe PID: 6096 Parent PID: 5292

General

Start time:	19:58:00
Start date:	11/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: schtasks.exe PID: 3708 Parent PID: 4088

General

Start time:	19:58:01
Start date:	11/06/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'schtasks.exe' /create /f /tn 'DHCP Monitor Task' /xml 'C:\Users\user\AppData\Local\Temp\tmpFE1B.tmp'
Imagebase:	0x8d0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

File Read

Analysis Process: ws8W4yPAvg.exe PID: 3012 Parent PID: 528

General

Start time:	19:58:01
Start date:	11/06/2021
Path:	C:\Users\user\Desktop\ws8W4yPAvg.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\ws8W4yPAvg.exe 0
Imagebase:	0x50000
File size:	207872 bytes
MD5 hash:	4F777AC67C52BE4D6A8B6F125BC94661
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000002.223088157.0000000000052000.00000002.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000002.223088157.0000000000052000.00000002.00020000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000005.00000002.223088157.0000000000052000.00000002.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000002.224117894.00000000038B1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000005.00000002.224117894.00000000038B1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000002.224074695.00000000028B1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000005.00000002.224074695.00000000028B1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000000.209534119.0000000000052000.00000002.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000000.209534119.0000000000052000.00000002.00020000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000005.00000000.209534119.0000000000052000.00000002.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: conhost.exe PID: 5396 Parent PID: 3708

General

Start time:	19:58:02
Start date:	11/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: dhcpmon.exe PID: 3216 Parent PID: 528

General

Start time:	19:58:03
Start date:	11/06/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' 0
Imagebase:	0x390000
File size:	207872 bytes
MD5 hash:	4F777AC67C52BE4D6A8B6F125BC94661
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000000.214551753.0000000000392000.00000002.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000000.214551753.0000000000392000.00000002.00020000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000007.00000000.214551753.0000000000392000.00000002.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000002.229264984.00000000029E1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000007.00000002.229264984.00000000029E1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000002.229298937.00000000039E1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000007.00000002.229298937.00000000039E1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000002.228024538.0000000000392000.00000002.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000002.228024538.0000000000392000.00000002.00020000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000007.00000002.228024538.0000000000392000.00000002.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: dhcpmon.exe PID: 3528 Parent PID: 3388

General

Start time:	19:58:07

Start date:	11/06/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe'
Imagebase:	0xc0000
File size:	207872 bytes
MD5 hash:	4F777AC67C52BE4D6A8B6F125BC94661
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000002.239146095.00000000036A1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000008.00000002.239146095.00000000036A1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000008.00000002.238181318.00000000000C2000.00000002.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000002.238181318.00000000000C2000.00000002.00020000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000008.00000002.238181318.00000000000C2000.00000002.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000008.00000000.222145161.00000000000C2000.00000002.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000000.222145161.00000000000C2000.00000002.00020000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000008.00000000.222145161.00000000000C2000.00000002.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000002.239109730.000000000026A1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000008.00000002.239109730.000000000026A1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities Show Windows behavior

File Created

File Read

Disassembly

Code Analysis